International Journal of Computer Science Engineering
and Information Technology Research (IJCSEITR)
ISSN(P): 2249-6831; ISSN(E): 2249-7943
Vol. 6, Issue 2, Apr 2016, 51-62
© TJPRC Pvt. Ltd.

TRANS STELLAR
•Journal Publications •Research Consultancy

FACE RECOGNITION SYSTEM USING BIO METRICS & SECURITY

V.S.MANJULA

Associate Professor, Department of Computer Science & Engineering, St. Joseph University College of Engineering & Technology, Dar-Es-Salaam, Tanzania, East Africa

ABSTRACT

Face recognition technology has received much attention due to its application in defense and crime prevention. Face recognition has a goal of computer vision, and become a realistic aim of biometrics research. Biometrics-based Authentication to identify the weak links in systems employing biometrics authentication, and present new solutions for eliminating of these weak links. For illustration purpose finger print authentication is used throughout, our analysis to extends biometrics based techniques. In such applications, there is great need to incorporate face recognition technologies to allow the spot field usage. New algorithms are used and developed by using cameras and increasing availability processing power has led to practical face recognition systems. Existing methods do not solve all the problems. In this method has high compression ratio and the compressed image can be easily stored in the database. Face recognition algorithms can be executed directly and without decompression. The security and privacy method is addressed by prune most DCT coefficients of images and by a random permutation protocol.

KEYWORDS: Facial Expressions, Human Machine Interaction, Training Sets, Expression Recognition, DCT & Neural Networks.

Received: Mar 08, 2016; **Accepted:** Mar 22, 2016; **Published:** Apr 07, 2016; **Paper Id.:** IJCSEITRAPR20167

Original Article

INTRODUCTION

Recognizing faces are effortlessly and without conscious thought, it has a difficult problem in the area of computer vision and finding technological solutions. Biometric technology are used face recognition and it has a number of problems solved with using research methodologies. The problem of face recognition can be stated as ‘identifying an individual person” as part of the battle against terrorism and criminal elements, efforts are currently under way to improve internal security through various measures. For this reason, the German Prevention of Terrorism Act of January 2002 introduced a number of amendments to the German Passport Act and Identity Card Act. These enable identity documents to be extended to incorporate biometric characteristics such as face, fingerprint or hand geometry, with a view to improving the process of determining a person's identity. Moreover, central storage of these biometric characteristics is not allowed. This makes it a priority to use biometric methods in the verification mode comparison of a characteristic stored in the identity card against the corresponding live characteristic of the person. It is important of biometrics-based authentication systems be designed in security in large-scale authentication systems.

Spur

The facial recognition on personal document systems from prescribed method in order to ensure interoperability. Moreover, it contains photographs for both the identity card and the passport its present form information. The basic method of biometric facial characteristics on the ID card that might be considered the

existing photograph and to be stored in a database and integrated in facial identity. The Bio Application of face recognition system examined the feasibility and technical implementation issues that arise in the following connection.

- Security agencies make use of face recognition products to catch suspects on the basis of their facial identity.
- Law enforcement bodies also use these products to catch criminals on run.
- Airline industry is another field, where these products are installed to avoid hijacking and other criminal activities.
- Banks and government offices also use face recognition technology to restrict undesirable happenings.

In addressing the underlying international situation, facial images that can be used with biometric systems have been considered. The basic biometric study facial recognition systems tested and comparing facial algorithms using verification modes. The decision has been taken of this system using selection test carried out of actual trials.

Advantages of Face Recognition System

Face recognition products offer low-cost high-profile security and that too, without hindering the normal working of an organization. These products are of great use in congested areas, where it becomes difficult to keep an eye on every individual. Easy to integrate with present security system, these products can perform well in internal as well as external environments. Can also be used for visitor tracking to help in investigation at the site of crime. The Bio PI study was carried out under the direction of the BSI and which was responsible for overall the project. The study was performed under contract by secunet Security Networks AG. This document is the official final report for the Bio PI study.

Secunet

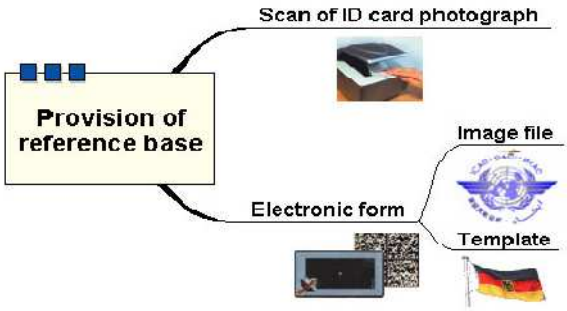

Figure 1: Provision of Reference Photographs for Facial Recognition

To evaluate these methods with their suitability method for facial recognition and using different reference bases tested.

Facial Recognition System Parameters

Face recognition the following parameters were determined prior to the start of the field test for both systems and were not subsequently altered during the trial.

- **Master Reference:** System template generated during live enrolment was chosen as the reference base, against whose template the live image was subjected to verification during the interactive equipment activation.
- **Master Algorithm:** Algorithm was chosen as the matching engine with which the live image was checked against the master reference during the interactive equipment activation. This algorithm was used in both systems.

- **Tolerance Threshold:** The threshold method was to finding the final decision and the match score from which verification was considered successfully. The choice of tolerance threshold initially followed by the recommendations of the vendors. In the pilot trial it turned out that when the same tolerance thresholds were used and the system produced better recognition performance. To exclude the possibility of the threshold influencing the user surveys which were carried out in parallel to the field test, it was decided and the systems should have similar recognition performance for user feedback.
- **Timeout on Recording the Live Image:** The maximum time was set for live images to six seconds during which the data acquisition unit continuously recorded.

In Figure 1 show that on the ID card the photograph can be used as the reference. During identity verification of a person, the photograph on the ID card is scanned and compared with the new image generated during identity verification. This type of ID card, the photograph contains different characteristics. This can be either an image file of the face or a special proprietary encoding of the face. During identity verification, the reference base would be read from this memory area. In a formal sense, biometrics refers to any automatically measurable, robust, and distinguished physical characteristic that can be used to identify an individual person.

RELATED WORK

Face Recognition Algorithms

There has been a rich body of work on face recognition algorithms. These algorithms typically first extract some important features from images. Principal component analysis (PCA), Independent Component Analysis (ICA), Evolutionary Pursuit (EP), Kernel-based methods as well as Bayesian Learning methods are also proposed. Of all these methods, variants of the PCA and ICA based methods are the most well known, well established and most commonly used. Some authors suggested the use of Discrete Cosine Transform feature vectors or different types of wavelets such as Gabor features instead of PCA.

Principle Component Analysis are used to convert the image and calculated on highly correlated image data. Once image features are extracted, a variety of classification techniques are used such as Hidden Markov Models, Neural Networks, Support Vector Machines, nearest neighbor match are used for the recognition process. Of all these, the nearest neighbor approach is the simplest, highly efficient, and most commonly used one.

Biometric Security Overview

Biometric Authentication method can be used in security and access control to measurable physical characteristics of a person. The verification of these photographs that can be checked automatically. Though you may not think about some specific biometric identifications, such as your driver's license contains biometric information about you. In this method calculated the person’s face shape, skin color, height, weight, hair color, nose tips and eye color for all physical characteristics that can be easily verified. However, your height changes according to your age for example 16 year old drivers get taller or shorter, if you are wear colored contact lenses that can change your eye color and hair color changes naturally.Biometric data that does not change they look for physical characteristics that stay constant and to find difficulties of changes of hair color and pose characteristics and fake and to change way of dressing styles. Most of us can remember when biometric security checks were the stuff of science fiction or action movies.

Smart Cameras

A smart camera or intelligent camera is a vision system, in addition to image capture circuitry, is capable of extracting application-specific information from the captured images, along with generating event descriptions that are used in an intelligent and automated system. A smart camera is a self-contained; standalone vision system with built-in image sensor stores the captured image in the memory. It transfers the digital image to another device using necessary communication interfaces. In the past, a typical camera was only able to capture images. Now, the smart camera will have the ability to generate specific information from the images that it has captured and well-established definition to be given what exactly a smart camera is. In this paper, we define a smart camera as a vision system which can extracted features from images and generate specific information for other devices such as PC or surveillance system.

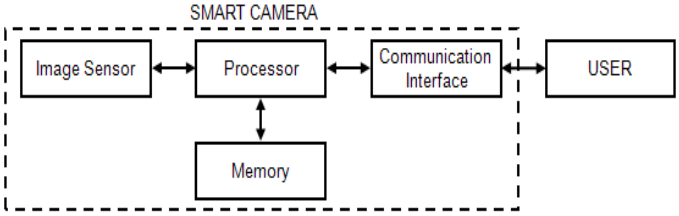

Figure 2: Shows a Basic Structure of a Smart Camera

It is intuitive, even though somewhat less flexible, development tools where existing functionalities can be connected in a list. Many development tools are available with relatively little but comparatively high level functionality, which can be configured and deployed with very limited effort. However, unlike the simple processor in a typical digital camera, the processor in a smart camera to control the camera functionalities, and to analyze the captured images to obtain extra information.

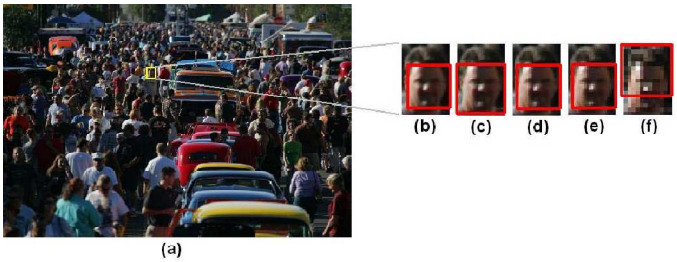

Figure 3: Overall Scene (a), ROI extracted from scene with Resolution of 7MP (b), 5MP(c), 3MP (d), 1MP (e) and VGA (f)

CMOS image sensor offers high resolution and low noise output. Due to the low power and high speed of CMOS, it is outperform CCD based image sensors. There are many CMOS image sensors in the market like Omni Vision, Micron and Kodak. It is noticeable that the frame rate is inversely proportional to the resolution of the camera. For wide angle surveillance, since no rapid movements of object of interest are expected, 5 high resolution frames per second can be considered as acceptable baseline performance for the prototype.

PHYSICAL BIOMETRIC TECHNIQUES

Fingerprinting

Biometric techniques have allowed law enforcement to improve on fingerprinting using biometric. The technological using advanced methods in fingerprinting had a major impact on identifying prints at crime scenes and

recording them from a person's characteristics. Now a day this method most popular in physical technique, and it is used to identify the person's ID cards, as the employee's hand is the only required information. For example if we take an image of a person are fingertips and record shows its characteristics. The patterns are matched or encoded and then compared with other fingerprint records. Although with digital scanning method is preferred for identifying them. With this digital scanning, a user presses his or her finger gently against a small optical or silicon reader surface where fingerprint information is taken from the digital scan and sent to a database for verification and identification comparison.

Figure 4: (a) Physical Security

Now a day's many places Biometrics are capitalizing on the competitive and dynamic fingerprint market with the development and innovation of physical security. In Figure 4(a) fingerprint security readers provides a piece of mind in having no passwords or PIN numbers to remember. Pin numbers can also be used with either Biometric system or a disability that makes hand or fingerprint reading impractical or impossible. In this method is flexibility and interoperability for administrators because an unlimited number of users are using this machine and it is ease of use and compatibility with all major access control systems. In addition, a large number of banks will incorporate this as the accepted authorization at ATMs for withdrawing and depositing money for fingerprint scan checkout and registered user's credit card or debit account. However the possibility of tricking the system with fake fingerprints is verified from the database. The future of fingerprinting appears to be very bright, as you will continue to see widespread usage within the law enforcement community and for personal use.

Figure 4: Casio Cellular Scanner

Today, BIO-key operates on a series of accessory fingerprint reader connections that operate on the iOS platform. Our software also operates directly on the device of certain Android and Win Mobile Smart Phones. In future many companies such as Apple, Samsung, LG and Google are all planning to introduce fingerprint sensors on their devices. BIO-key will seek to deliver integrated solutions for every device, consistent with the company business model which calls for universal interoperability.

We anticipate that there will be many developments involving mobile devices, incorporating biometric technology in the coming months. BIO-key is the only fingerprint biometric developer that can claim universal interoperability. Our technology is used by hospitals, blood centers, call centers, testing centers, schools, retailers, and enterprises, along with federal and international government agencies. BIO-key to be an innovative mobile authentication partner, providing these services and many more:

- Mobile cloud authentication
- Eliminate the use of cumbersome passwords
- Streamline access to privileged information
- Operates on any platform including iOS, Android and WinMobile
- One enrollment enables you to authenticate on any approved device & mobile

Facial Recognition

Face VACS-Entry technology facial recognition scanner is used to scanning the person's face and identifying the person.Figure 5(a) shows the most recent technology is used to airport access passenger physical part of face and irish verified. In an effort to speed up travelers' passage through airports, a electrical systems company has come up with robots, it specializes in electrical systems for the aerospace, defense and security sectors. Passengers won't have to deal with check-in desks, as to scan passports and print boarding passes. The technology, which is already using in many airports, the machine tells to record an image of the passenger's face and of their irises. The biometrics will be used to confirm the passenger's identity and then shared with computers around the airport. An encrypted image of the person's face would also be printed on boarding passes to enhance safety and produces biometric passports and IDs.

Figure 5: (a) Face Scanning

Figure 5: (b) Time Masters Hand Punch

Figure 5(b) shows Time Masters Hand Punch machine, used Corporate Companies have specialized in this technology and have marketed hand and finger geometry as a part of a workforce management solution. The Time Masters Hand Punch captures a three-dimensional accurate image of an employee's hand each time an employee punches in and out with green and red lights notifying the employee of the status of each punch. 8D FDB5 DE3D 8B6

Iris Scanning

Now a day's Iris scanning is used in many places to verifying and recognition of the person's face. In Iris features the colored tissue surrounding the pupil of an eye. It involves a user, as close as a couple of inches and up to 2 feet away, looking into a device where their iris is scanned and compared. The comparison is conducted at more than 200 points and checked for similar rings, furrows and freckles of the eye. The main advantage of iris scanning involves the extreme accuracy of the technology. Since no two irises are similar, identification and verification are done with confidence. Iris scanning also involves non-invasive technology; an ease of use since irises cannot be stolen, unlike keys, access cards, and password systems; and eliminates the frustration for users to have to remember passwords. In addition, the other techniques learned thus far, will recognize a fake eye from a real one by varying the light shone into the eye and watching for pupil dilation. The main challenge of iris scanning involves its high cost.

Figure 6: Irish Scanning Process

Additional challenges involve the potential difficulty in getting someone to hold their head in the right spot for a scan, bad readings due to poor. In this machine mainly used Airports & Corporation follow this Iridian Technologies have taken iris scanning with the development of their very own proprietary architecture and camera software. In these technology licensees such as Panasonic, Oki, and LG and Iris Scanners – Windows based Workstation iris scanner.

Retinal Scanning

Retinal scanning is the most accurate physical biometric technique that uses the unique patterns on a person's retina. Similar to iris scanning, retinal scanning to analyze the layer of blood vessels light more readily than the surrounding tissue, the amount of reflection varies during the scan.

Figure 7: Scanning Physical Process

The scanning involves using a low-intensity light source and an optical coupler that reads the patterns of a person's retina. Still relatively new and primarily used for high-risk security areas, its popularity is gaining acceptance. Retinal scanning has a user look through a small opening in the device at a small green light. The user must keep their head still and eye focused on the light for several seconds during which time the device will verify his or her identity. This process takes about 10 to 15 seconds total. Besides being the most accurate biometric technique available, retinal scanning provides for several additional advantages. The first advantage is the capability of providing viewing assistance to those who are visually impaired; a second advantage is providing a piece of mind in knowing the technology is 100% accurate, and the final advantage of the technology being seen as a great long term cost alternative to some other biometric techniques. In addition several challenges to this technology exist. They include the invasive screening process and user discomfort.

Figure 8 (a): Original

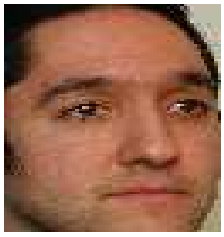

Figure 8 (b): Testing Image

For example, it requires a user to stand within inches of a device to get an accurate reading, it requires a user to remove glasses if they wear them, it requires a user to place their eye close to the retinal scanning device, and it requires a user to focus on a certain point for a certain period of time. The future of retinal scanning appears bright. However, it needs to be more refined, non-intrusive, and cost effective for acceptance.

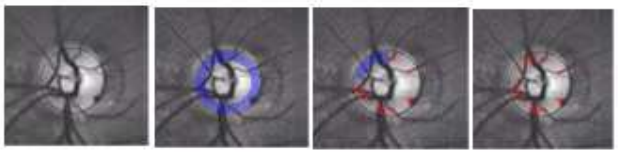

Figure 9: Retinal Tech Scanning Process

To illustrate the retinal scanning process, Retinal Tech Corporation offers a retinal scanning device that scans a person's retina in four distinct and different phases. This technology is designed to be extremely versatile for attachment to a door for physical access, incorporation into a wand, kiosk, or ATM machine, and for connection to a computer. It also works outdoors, in low lighting, and is hands free.

IMPLEMENTATION OVERVIEW

The main obstacles of biometrics will continue to involve complexity and privacy issues surrounding information abuse. Biometric information has abused by the risks posed and how this information can be misused for unimaginably evil purposes by other people, employers, and governments. Additional concerns center around biometric accuracy and performance vendors need to be able to commit to a 100% accuracy of their technologies, something that they do not want to do at this time. In Biometric techniques are easy to hoodwink such as the case of a fingerprint saved on a piece of candy and systematic bypass of determined and creative hackers. In other words, today's hacker is becoming smarter than ever. Physiological biometric technology and finger scan technology (36%) will continue to dominate the biometric market. However, other technologies such as hand 27%, signature 5%, iris 16%, voice 6%, and facial 11% recognition are all gaining popularity. And handwriting technology is becoming popular with banks and credit card authorizations. The future of biometrics depends upon its industry.

Biometrics usage will work with security software (firewalls, antivirus, and encryption) and security hardware (token and smart cards, and firewall devices). In security sensitive environments such as airports and casinos; with law enforcement; prisons, jails, amusement and theme parks, corporate time systems, in assisting the disabled and mentally challenged. The new technologies are communicating with a corporate network and more vendor product and service line expansion. The popularity of e-business will continue to be the driving force behind advanced security needs. When choosing a biometric system can be considered such as speed, accuracy, user-friendliness, low-cost, public acceptability, reliability, acceptable storage requirements, and fast enrollment times should all be considered.

Overall, I hope this paper has exposed to a vast future of opportunity that exists in physical security. The intent was to showcase and discuss the numerous biometric techniques available today and tomorrow, highlights the advantages and disadvantages of these techniques, illustrate key company and contact information if interested in implementing them, and to provide assistance and considerations with choosing the right biometric solution.

EXPERIMENTAL RESULTS

In this paper mainly considers the type of attacks where the device is stolen and someone tries to recover images stored on the device. The protection comes from the pruning of most DCT coefficients and the random permutation protocol. The DCT coefficients to get back the original data without knowing the random permutation order in which DCT-H shuffles the coefficients. The other transforms of principal component analysis, it is very difficult to decide the order based DCT coefficients . The size of image is typically pretty big while the number of coefficients selected (μ) is pretty small μ = 10). The denominator in Equation in such case will be big enough making the probability for the worst case scenario extremely small.


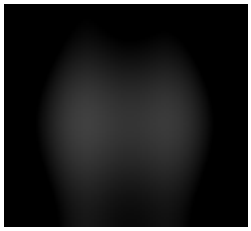

Figure 10 (a): Original **Figure 108 (b): Reconstructed**

The number of coefficients required for an accurate recognition task is much smaller than the number of coefficients needed to reconstruct an image that can be recognized by human being. Thus the images reconstructed from the compressed database have very poor quality. For example, Figure 10 (a) shows an original image and Figure 10 (b) shows an image reconstructed DCT coefficients. The reconstructed image is clearly not recognizable the permutation protocol is cracked. The image one can check out if it is in the compressed database through a nearest neighbor match. Actually there is no way to prevent encrypted the image, the device which will incur significant computational overhead resulting from the decryption required for the face recognition task. However it will be impossible to visually inspect any other images in the database..

Face Authentication will use face recognition technologies to analyze and determine on the system. This paper reported on our prototype development of a smart camera for automated face recognition using high resolution (5MP) sensors. The smart camera extracts all the faces from the full-resolution frame and only sends the pixel information from these face areas are shown to the main processing system. The main challenge in this project is to build a stand-alone and low power smart camera system that integrates real-time face detection for crowd surveillance.

Table 1

Error Rate	Value Range	Evaluation According to Criterion Catalogue
FAR	< 0.3%	Very high
	0.3% - 1%	High
	1% - 5%	Moderate
	> 5%	Low
FRR	< 1%	Very high

	1% - 3%	High
	3% - 7%	Moderate
	> 7%	Low

Algorithm comparison and reference base comparison using the recognition performance of a biometric system always has to be stated as a combination of FRR and FAR. To compare the algorithms and working points were determined; these points could be oriented to fixed values of either the FAR or the FRR. The main focus of this paper show interest and used various aspects of security.

CONCLUSIONS

Face recognition is a technology just reaching sufficient maturity for it to experience a rapid growth in its practical applications. Crime and crime policy are complex but important areas of research. In this article, I have tried to highlight what we know about the determinants of crime and outlined a number of issues which we need to understand in order to design an effective crime policy. Smart Cameras are slowly being introduced in emerging surveillance systems. The decision to commit crime depends on a number of factors, but at least some of them can be identified with careful analysis. Given the huge impact that crime has on societal welfare, analyzing the determinants of crime is an important research agenda with very clear policy implications. But care needs to be taken as causal identification is not easy to do and looking at correlations from raw data can be misleading. Thus, there is a need for rigorous quantitative analysis. Our own analysis suggests that policing interventions are important determinants of crime rates while frequently cited economic and social factors are not so closely linked.

REFERENCES

1. *Woodward, John. "Biometrics: A look at Facial ,Recognition";October2003.http://www.rand.org/publications/DB/DB396/DB396.pdf*
2. *Individual Biometrics. "An Overview of Biometrics", June 2002 http://ctl.ncsc.dni.us/biomet%20web/BMIndex.html,*
3. *Precise Biometrics. "Personal Proof: Knowing who's who when security really counts", November 2003.http://www.precisebiometrics.com/data/content/DOCUMENTS/200359141 913709Personal_Proof_2003.pdf*
4. *Biometric Security Systems. "Biometric Technologies", November 2003. http://www.biometricsecurity.com.au/technologies/technologies.htm*
5. *Williams, Martyn. "Casio Unveils Better Cell Phone Security",http://pcworld.shopping.yahoo.com/yahoo/article/0,aid,109597,00.asp, Yahoo; Feb 28, 2003.*
6. *Sebastien Marcel and Yann Rodriguez, "Biometric Face Authentication using Pixel-based Weak Classiers"*
7. *Penman, Richard. "The Role of Facial Recognition: Biometrics in the Security Industry", Geocities, July 6, 2002.http://www.geocities.com/penmanre/Research/FacialRecognitionBiometrics.htm*
8. *A. J. Goldstein, L. D. Harmon, and A. B. Lesk, "Identification of human faces" – 1971*
9. *Ching-Han CHEN,Chia -Te CHU, "Face Authentication System for Information Security".*
10. *W. Du and M. J. Atallah. Secure multi-party computation problems and their applications: a review and open problems.In 2001 Workshop on New Security Paradigms, pages 13–22, Cloudcroft, NM, 2001.*
11. *R. Duda and P. E. Hart. Pattern classification and scene analysis. John Wiley & Sons, 1973. K. Chen and L. Liu. A random rotation perturbation approach to privacy-preserving data classification. In IEEE Intl. Conf on Data Mining 2005, Houston,*

Tx, November 2005.

12. *P. Jonathon Phillips, Hyeonjoon Moon, Patrick Rauss, and Syed A. Rizvi. The FERET September 1996 Database and Evaluation Procedure. In Josef Big¨un, G´erard Chollet, and Gunilla Borgefors, editors, Audio- and Video-based Biometric Person Authentication, Volume 1206 of Computer Science, pages 395–402. Springer, March 1997.*

APPENDIX

Author Profile

Dr.V.S. Manjula has Completed MCA, M.Phil., B.Ed., DTE, Ph.D and She received Ph.D degree in Computer Science from Bharathiar University in 2013. She worked in Head in MCA Department, Gurushree Shantivijai Jain College, Chennai. At present she is working in Associate Professor in the Department of Information System and Network Engineering & Computer Science Engineering in St. Joseph University College of Engineering & Technology, Dar-Es-Salaam in Tanzania, East Africa. She is a Research Supervisor in Information & Communication Technology (ICT) in St. Eugene University in Zambia and she is a member of Research Journal of International Association of Computer Science & Information Technology (IACSIT). She has published more than 12 International Journals and National & International Conferences.